MANAJEMEN RISIKO ASET PERANGKAT IT PADA DISKOMINFO STATISTIK DAN PERSANDIAN KOTA XYZ MENGGUNAKAN STANDAR ISO/IEC 27005: 2008

Tugas Akhir

Diajukan untuk memenuhi persyaratan mencapai derajat Sarjana Sistem Informasi

Enjel Simanjuntak

161709068

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ATMA JAYA YOGYAKARTA

2021

LEMBAR PENGESAHAN

Tugas Akhir Berjudul

MANAJEMEN RISIKO ASET PERANGKAT IT PADA DISKOMINFO STATISTIK DAN PERSANDIAN KOTA XYZ MENGGUNAKAN STANDAR ISO/IEC 27005: 2008

Yang disusun oleh

ENJEL SIMANJUNTAK

161709068

dinyatakan telah memenuhi syarat pada tanggal 10 Februari 2021

		Keterangan
Dosen Pembimbing 1	: Prof. Ir. A. Djoko Budiyanto, M.Eng., Ph.D.	Telah menyetujui
Dosen Pembimbing 2	: Prof. Ir. A. Djoko Budiyanto, M.Eng., Ph.D.	Telah menyetujui
Tim Penguji		
Penguji 1	: Prof. Ir. A. Djoko Budiyanto, M.Eng., Ph.D.	Telah menyetujui
Penguji 2	: Yohanes Priadi Wibisono, S.T.,M.M.	Telah menyetujui
Penguji 3	: Clara Hetty Primasari, S.T., M.Cs	Telah menyetujui

Yogyakarta, 10 Februari 2021

Universitas Atma Jaya Yogyakarta

Fakultas Teknologi Industri

Dekan

ttd

Dr. A. Teguh Siswantoro, M.Sc

LEMBAR PERNYATAAN
Orisinalitas & Publikasi Ilmiah

Saya yang bertanda tangan di bawah ini:

Nama Lengkap	: Enjel Simanjuntak
NPM	: 161709068
Program Studi	: Sistem Informasi
Fakultas	: Teknologi Industri
Judul Penelitian	: MANAJEMEN RISIKO ASET PERANGKAT IT PADA DISKOMINFO STATISTIK DAN PERSANDIAN KOTA XYZ MENGGUNAKAN STANDAR ISO/IEC 27005: 2008

Menyatakan dengan ini:

1. Skripsi ini adalah benar merupakan hasil karya sendiri dan tidak merupakan salinan sebagian atau keseluruhan dari karya orang lain.
2. Memberikan kepada Universitas Atma Jaya Yogyakarta, berupa Hak Bebas Royalti non eksklusif (*Non-Exclusive-Royalty-Free Right*) atas Penelitian ini, dan berhak menyimpan, mengelola dalam pangkalan data, mendistribusikan, serta menampilkan untuk kepentingan akademis, tanpa perlu meminta izin selama tetap mencantumkan nama penulis.
3. Bersedia menanggung secara pribadi segala bentuk tuntutan hukum yang mengikuti atas pelanggaran Hak Cipta dalam pembuatan Skripsi ini.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 25-01-2021
Yang menyatakan,

Enjel Simanjuntak
161709068

PRAKATA

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena berkat rahmat-Nya, penulis dapat menyelesaikan penulisan tugas akhir "Manajemen Risiko Aset Perangkat IT pada DISKOMINFO STATISTIK DAN PERSANDIAN Kota XYZ Menggunakan Standar ISO/IEC 27005: 2008". Penulisan tugas akhir ini bertujuan untuk memenuhi syarat untuk mencapai derajat sarjana Sistem Informasi dari Program Studi Sistem Informasi, Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta. Penulis menyadari, bahwa dalam penulisan tugas akhir ini ada banyak bantuan, motivasi, dan masukan yang penulis dapatkan dari berbagai pihak, untuk itu penulis ingin mengucapkan terima kasih kepada:

1. Tuhan Yesus Kristus yang selalu melindungi dan membimbing penulis dalam berbagai kondisi
2. Bapak Prof. Ir. A. Djoko Budiyanto, M.Eng., Ph.D., selaku dosen pembimbing I senantiasa bersedia mengarahkan dan memberikan motivasi kepada penulis sejak dari proses awal penyusunan tugas akhir
3. Bapak Al. Bagas Pradipta, S.Kom., M.Eng., selaku dosen pembimbing akademik yang senantiasa memberikan motivasi dan bimbingan kepada penulis selama menempuh pendidikan di Program Studi Sistem Informasi
4. Seluruh dosen Program Studi Sistem Informasi
5. Pembimbing Lapangan di DISKOMINFO Statistik dan Persandian yang bersedia untuk direpotkan dan senantiasa membantu dalam penulisan tugas akhir ini
6. Kedua orang tua tercinta, Bapak Cirus Simanjuntak dan Ibu Justina Saragih yang selalu memberikan kasih sayang, dukungan doa maupun material kepada penulis selama menempuh pendidikan
7. Abang penulis, Sanipius Simanjuntak, yang selalu memberikan motivasi, memberikan dukungan doa dan material kepada penulis selama menempuh pendidikan
8. Sahabat-sahabat penulis, Marindah Ulfa, Aninda Milenia, Dian Sophia yang selalu setia memberikan semangat kepada penulis

9. Kepada Jerry, yang selalu memberikan dukungan semangat dan doa untuk penulis
10. Seluruh teman-teman Sistem Informasi 2016, yang bersama-sama berjuang dengan penulis dari awal perkuliahan
11. Dan kepada seluruh pihak yang tidak dapat penulis sebutkan satu persatu, penulis ucapkan terima kasih sebanyak-banyaknya

Demikian laporan tugas akhir ini dibuat semoga dapat bermanfaat bagi pembaca.

Yogyakarta, 25-01-2021

Enjel Simanjuntak

Penulis

ABSTRAK

Teknologi informasi merupakan bagian yang penting dan utama bagi sebuah organisasi karena dapat mendukung lancarnya proses bisnis organisasi. Berbagai organisasi telah bergantung pada teknologi informasi baik organisasi nonprofit ataupun profit termasuk Dinas Komunikasi Informatika Statistik dan Persandian Kota XYZ. Organisasi ini merupakan organisasi pemerintahan daerah yang menggunakan teknologi informasi sebagai komponen utama dalam proses bisnis karena tanggung jawab yang dimiliki organisasi adalah mengelola informasi yang ada di kota tersebut, maka dari itu diperlukan manajemen keamanan pada aset yang dimiliki sehingga risiko yang mungkin terjadi dapat diminimalkan kerugiannya dan tidak memberikan dampak besar pada jalannya proses bisnis. Dalam penelitian ini lebih spesifik pada salah satu aset yang dimiliki oleh organisasi yaitu aset perangkat IT. Untuk memenuhi kebutuhan keamanan aset informasi maka diperlukan dokumen manajemen risiko. Metode yang digunakan pada penelitian ini adalah metode penelitian kualitatif dengan pendekatan deskriptif. Penelitian ini menggunakan kerangka kerja ISO 27005:2008 sebagai acuan dalam proses manajemen risiko. Standar ini digunakan sesuai dengan anjuran dari pemerintah yang tertera dalam peraturan kementerian Kominfo RI. Standard ini mempunyai beberapa tahapan dimulai dengan mengidentifikasi aset kemudian melakukan klasifikasi terhadap aset berdasarkan standar ISO 27005:2008, kemudian menentukan risiko dan kerawanan yang mungkin terjadi dan langkah terakhir adalah melakukan evaluasi risiko dan memberikan rekomendasi. Berdasarkan proses manajemen risiko yang dilakukan pada penelitian ini dihasilkan 30 ancaman risiko dari 17 aset yang telah diklasifikasi, dari 30 ancaman risiko terdapat 24 risiko pada level *low*, 5 risiko pada level *medium* dan 1 risiko pada level *high*. Dari nilai yang sudah didapatkan maka dirumuskan rekomendasi untuk meminimalkan risiko yang mungkin terjadi di Diskominfo Statistik dan Persandian Kota XYZ dan rekomendasi ini diharapkan dapat diterapkan.

Kata Kunci: ISO 27005:2008, Manajemen Risiko, Keamanan Informasi, Penilaian Risiko, Aset Informasi

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I PENDAHULUAN

1.1. Latar Belakang

Pada era saat ini teknologi informasi terus berkembang dengan sangat cepat, oleh karena itu organisasi dituntut untuk selalu mampu beradaptasi dengan perkembangan tersebut[1]. Teknologi informasi memiliki peranan penting bagi sebuah organisasi dikarenakan peranan strategis itu mampu untuk meningkatkan kualitas pelayanan dan memberi dukungan pada proses bisnis dalam mencapai tujuan organisasi[2]. Teknologi informasi memberikan dukungan yang sangat besar pada sebuah organisasi yaitu dengan memberikan nilai tambah dan peningkatan efisiensi dan efektivitas pada pelaksanaan operasional organisasi. Di dalam teknologi informasi terdapat informasi yang memiliki nilai tinggi bagi organisasi dan menjadi aset yang sangat berharga, karena informasi ini dapat digunakan dalam pengambilan keputusan manajerial[3]. Dengan pentingnya peranan teknologi informasi tersebut maka perlu memperhatikan keamanan informasi dan aset penting organisasi, Namun yang terjadi pada saat ini banyak organisasi yang kurang memberikan perhatian khusus bagi keamanan informasi dan aset-asetnya[4].

Penggunaan teknologi informasi sangat meluas, salah satunya digunakan dalam lembaga pemerintahan atau organisasi yang menyelenggarakan pelayanan publik, hal ini bertujuan supaya kebutuhan akan layanan publik semakin efektif dan efisien. Kualitas layanan publik akan semakin meningkat dengan bantuan teknologi informasi dan sumber daya informasi yang terkandung didalamnya semakin mudah untuk disebarluaskan, hal ini merupakan bagian dari realisasi tata kelola pemerintahan yang baik[5]. Kemajuan teknologi informasi di lingkungan pemerintahan membentuk karakteristik baru dalam hal interaksi pemerintah dan juga masyarakat, yaitu dengan terbentuknya e-government yang memiliki konsep layanan publik dengan berbasis elektronik[6].

Pengembangan e-government sendiri yang ada di Indonesia didasarkan pada instruksi presiden RI Nomor 3 Tahun 2003 tentang kebijakan dan strategi nasional pengembangan e-government[7].

E-Government merupakan penggunaan teknologi informasi oleh lembaga pemerintahan dalam rangka berkomunikasi dengan masyarakat atau lembaga lainnya. E-Government bertujuan untuk meningkatkan transparansi, akuntabilitas, keefektifan dan keefisienan dalam rangka pelayanan publik dan penyelenggaraan pemerintahan[8]. Di sisi lain e-government memberikan tantangan baru bagi lembaga pemerintahan yaitu dari sisi keamanan informasi sehingga diperlukan pengelolaan teknologi informasi yang baik, seperti pada peraturan Menteri komunikasi dan informatika Nomor 41/PER/M.KOMINFO/11/2007 dinyatakan bahwa dibutuhkan perencanaan pengelolaan yang baik terhadap teknologi informasi sehingga dapat mendukung tujuan dari penyelenggaraan pemerintah terhadap pelayanan publik[9]. Keamanan informasi mengacu pada perlindungan aset informasi, karena adanya kemungkinan timbul ancaman-ancaman yang memberikan efek merusak pada fungsi lembaga administrasi publik dan menyebabkan terganggunya ketersediaan layanan publik[10]. Ada 3 aspek yang menjadi perhatian dalam keamanan informasi yaitu kerahasiaan, keutuhan dan ketersediaan. Untuk menghindari risiko dari ancaman yang mungkin terjadi, maka perlu adanya manajemen risiko pada setiap organisasi tidak terkecuali pada lembaga pemerintahan. Setiap organisasi membutuhkan pendekatan manajemen risiko yang akan dipimpin oleh pemimpin tingkat atas, hal ini akan didedikasikan untuk manajemen risiko dan keamanan informasi[11].

Melalui Kementerian Komunikasi dan Informatika, pemerintah telah membuat himbauan agar setiap lembaga pemerintahan meningkatkan kesadaran akan pentingnya keamanan informasi dengan cara penerapan manajemen keamanan informasi. Hal ini diatur dalam Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016

Tentang Sistem Manajemen Pengamanan Informasi pada Bab IV Pasal 10 Ayat 1 dikatakan bahwa "Penyelenggara Sistem Elektronik strategis dan Penyelenggara Sistem Elektronik tinggi wajib memiliki Sertifikat Sistem Manajemen Pengamanan Informasi" dan organisasi dapat melakukan penilaian secara mandiri dengan standar penilaian berdasarkan ISO 27000, hal ini disebutkan dalam Bab VII pasal 21[12]. Berdasarkan peraturan yang telah dijabarkan di atas dapat dilihat bahwa pemerintah saat ini sudah lebih responsif terhadap keamanan informasi. Namun masih ada organisasi yang belum menerapkan himbauan yang diberikan pemerintah pusat tersebut, salah satunya yaitu Diskominfo Statistik dan Persandian Kota XYZ. Diskominfo Statistik dan Persandian Kota XYZ merupakan salah satu instansi pemerintahan yang bertanggung jawab dalam pengolahan informasi di kota XYZ. Dinas Komunikasi Informatika Statistik dan Persandian Kota XYZ ini mengimplementasikan teknologi informasi untuk melaksanakan tanggung jawab tersebut, oleh karena ini perlu menerapkan keamanan informasi. Saat ini tingkat kepedulian organisasi dalam hal keamanan IT atau terkait manajemen risiko masih rendah. Keamanan IT dan keamanan informasi belum diperhatikan dengan baik, hal ini masih dianggap hal sepele oleh organisasi dan bukan suatu hal yang *urgent*. Kepedulian organisasi terhadap pentingnya manajemen risiko belum sepenuhnya baik, masih sedikit SDM yang mengerti dan paham tentang keamanan, karena pelatihan keamanan yang diberikan masih hanya untuk SDM bagian persandian dan hasil dari pelatihan belum sepenuhnya diterapkan. Untuk SDM yang belum mendapatkan pelatihan hanya dilakukan pemberian materi atau penjelasan dari pelatihan yang dilakukan oleh pihak persandian untuk menumbuhkan rasa kepedulian terhadap keamanan di dalam organisasi. Kurangnya perhatian dari organisasi terlihat dari pengendalian-pengendalian risiko yang dimiliki organisasi masih kurang, sehingga ketika terjadi kesalahan atau kerusakan dibutuhkan waktu lebih untuk perbaikan. Manajemen risiko keamanan informasi merupakan langkah yang dapat

dilakukan agar penerapan keamanan informasi pada organisasi dapat lebih efektif.

Manajemen risiko keamanan informasi merupakan proses yang terstruktur dan berkesinambungan yang memiliki tujuan untuk mengidentifikasi, mengevaluasi dan meminimalkan beberapa risiko yang berdampak negatif pada organisasi[13]. Dalam melakukan manajemen risiko terdapat beberapa standar yang dapat digunakan seperti FRAP, CRAMM, CORAS, Octave, NIST SP 800-30, ISO/IEC 27000[14][15]. Mengikut dari peraturan kementerian Komunikasi dan Informatika Republik Indonesia tentang manajemen pengamanan informasi pada pelayanan publik menggunakan ISO 27000 sebagai standar penilaian risiko. Pada penelitian ini menggunakan standar ISO 27005 yang merupakan salah satu bagian dari keluarga ISO/IEC 27000. ISO 27005 merupakan standar internasional yang memberikan panduan untuk manajemen risiko keamanan informasi.

1.2. Perumusan Masalah

Berdasarkan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi dikatakan bahwa pentingnya melakukan manajemen pengamanan informasi pada sebuah organisasi terlebih pada instansi pemerintahan yang menyelenggarakan pelayanan publik. Namun Dinas Komunikasi Informatika Statistik dan Persandian Kota XYZ belum sepenuhnya sadar akan pentingnya keamanan informasi dan belum menerapkan himbauan dari pemerintah tersebut. Belum adanya penerapan manajemen risiko keamanan informasi pada Dinas Komunikasi Informatika Statistik dan Persandian Kota XYZ dapat merugikan instansi, karena instansi belum siap mengolah bahkan menerima ketika muncul risiko yang mengancam keamanan informasi serta aset yang dimiliki. Hal ini dapat berdampak buruk pada pelayanan yang diberikan Dinas Komunikasi

Informatika Statistik dan Persandian Kota XYZ dan merusak nilai instansi ini di mata masyarakat.

1.3. Pertanyaan Penelitian

Berdasarkan rumusan masalah yang telah dijabarkan di atas maka dapat di rumuskan pertanyaan penelitian sebagai berikut:

1. Bagaimana melakukan manajemen risiko pada aset perangkat IT yang ada pada Diskominfo SP Kota XYZ?

1.4. Tujuan

Tujuan yang ingin diperoleh dari penelitian ini adalah:

1. Melakukan penilaian risiko aset perangkat IT melalui identifikasi risiko yang di Dinas Komunikasi Informatika Statistik dan Persandian Kota XYZ.
2. Memberikan rekomendasi pengamanan yang sesuai dengan standar manajemen risiko pada risiko yang telah diidentifikasi

1.5. Batasan Masalah

1. Penelitian ini menggunakan standar ISO 27005:2008 sebagai *best practice* manajemen risiko.
2. Penelitian berfokus pada penilaian risiko pada aset perangkat IT atau perangkat keras dari organisasi**.**

1.6. Manfaat Penelitian

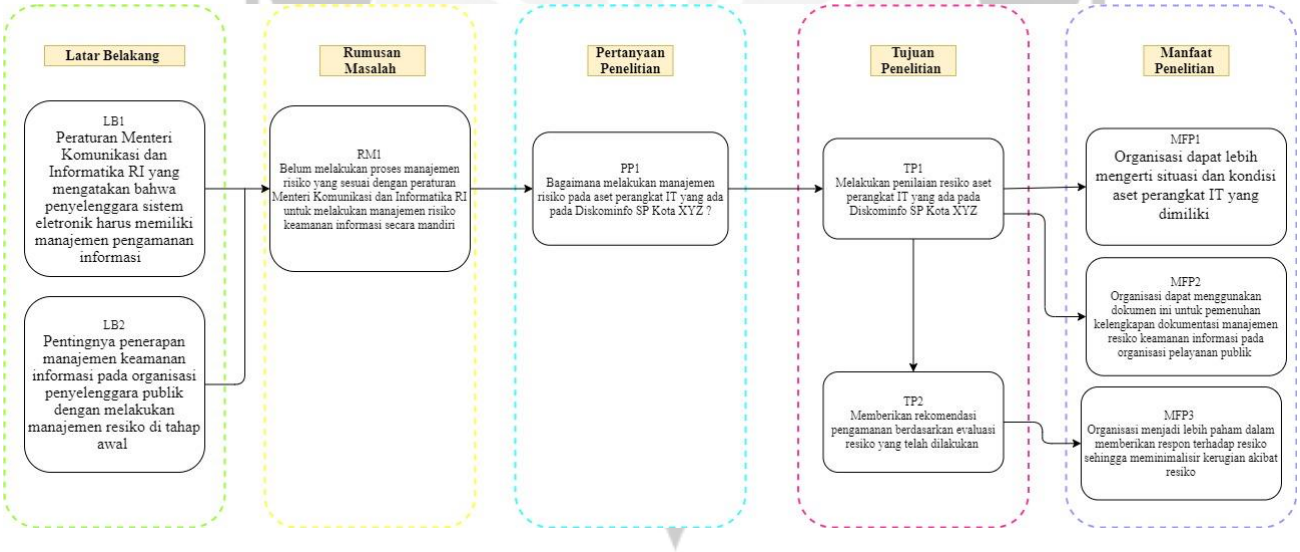
Manfaat yang ingin diperoleh dari penelitian ini adalah:

1. Organisasi dapat lebih mengerti situasi dan kondisi aset-aset yang dimiliki terutama pada aset.

2. Organisasi dapat menggunakan dokumen ini untuk pemenuhan kelengkapan dokumentasi manajemen risiko keamanan informasi pada organisasi pelayanan publik.

3. Organisasi menjadi lebih paham dalam memberikan respon terhadap risiko sehingga meminimalisir kerugian akibat risiko tersebut.

1.7. Bagan Keterkaitan



Gambar 1. 1 Bagan Keterkaitan

BAB V KESIMPULAN DAN SARAN

5.1. Kesimpulan

Proses penilaian risiko diawali dengan melakukan identifikasi aset secara keseluruhan yang ada di Diskominfo Statistik dan Persandian Kota XYZ, kemudian dilanjutkan dengan klasifikasi aset perangkat IT dengan menggunakan standar ISO 27005:2008 dan yang terakhir yaitu memberikan rekomendasi. Dari proses identifikasi awal terdapat 18 aset perangkat IT yang dimiliki oleh organisasi, kemudian aset ini diklasifikasikan berdasarkan ketentuan yang ada pada ISO 27005:2008 sehingga menyisakan 17 aset dikarenakan satu aset tidak memiliki kualifikasi yang cocok dengan ketentuan pada ISO 27005:2008. Dari 17 aset ini kemudian dilakukan identifikasi risiko dan menghasilkan 30 risiko. 30 risiko tersebut kemudian dikategorikan lagi ke 3 tingkat kategori level risiko yaitu *low*, *medium* dan *high*. Level risiko ini merupakan hasil dari nilai kecenderungan dan juga dampak yang sesuai dengan parameter yang telah dibuat.

Rekomendasi yang dibuat peneliti pada dokumen ini didasarkan pada tingkat risiko dan implementasi yang telah diharapkan. Untuk sebagian besar hanya perlu meningkatkan keamanan seperti melakukan peninjauan atau pengecekan secara berkala pada alat-alat yang dimiliki dan juga salah satu yang penting adalah melakukan pelatihan untuk meningkatkan kesadaran SDM akan pentingnya keamanan informasi, baik internal ataupun eksternal.

5.2. Saran

Berdasarkan keterbatasan dalam penelitian ini, berikut beberapa hal yang dapat diperhatikan untuk penelitian selanjutnya,

a. Sebaiknya peneliti turun langsung ke lapangan untuk mengawasi pada saat pengisian kuesioner sehingga hasil yang diharapkan dapat lebih optimal

b. Peneliti sebaiknya tidak hanya mengandalkan kuesioner tetapi untuk memenuhi kuesioner dapat lebih banyak mencari tahu keadaan organisasi secara riil.

c. Membuat kerangka penanganan risiko dengan memperhitungkan biaya pemulihan, level dan transfer risiko. Penanganan ini dilakukan pada risiko yang tidak dapat ditangani oleh pengendalian saat ini secara efektif.

DAFTAR PUSTAKA

[1] E. R. Pratama, Suprapto, and A. R. Perdanakusuma, "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001: Studi Kasus KOMINFO Provinsi Jawa Timur," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 5911–5920, 2018, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3465.

[2] R. Budiarto, "Manajemen Risiko Keamanan Sistem Informasi," vol. 2, no. 2, pp. 105–115, 2017, doi: 10.24114/cess.v2i2.6264.

[3] H. Susanto, M. Almunawar, and Y. Tuan, "Information security management system standards: A comparative study of the big five," *Int. J. Electr. Comput. Sci. IJECS-IJENS*, vol. 11, no. 5, pp. 23–29, 2011.

[4] D. Rachmawan, A. Pribadi, and E. Tyas D., "Pembuatan Dokumen Sop Keamanan Aset Informasi Yang Mengacu Pada Kontrol Kerangka Kerja Iso 27002:2013 (Studi Kasus : Cv Cempaka Tulungagung)," *J. Tek. ITS*, vol. 6, no. 1, pp. 192–197, 2017, doi: 10.12962/j23373539.v6i1.21369.

[5] A. B. Setiawan, "Kajian Kesiapan Keamanan Informasi Instansi Pemerintah Dalam Penerapan E-Government," *J. Masy. Telemat. dan Inf.*, vol. 4, no. 2, pp. 109–126, 2013.

[6] R. Ihmouda, N. H. Mohd Alwi, and I. Abdullah, "A Systematic Review on E-government Security Aspects," *Int. J. Enhanc. Res. Manag. Comput. Appl.*, vol. 3, no. 6, pp. 60–67, 2014.

[7] I. Presiden, R. Indonesia, K. Dan, S. Nasional, P. E-government, and P. R. Indonesia, *Instruksi Presiden Republik Indonesia*. Indonesia, 2003.

[8] S. Romayah, A. I. Suroso, and A. Ramadhan, "Evaluasi implementasi E-Government di Instansi XYZ," *J. Apl. Manaj.*, vol. 12, no. 4, pp. 612–620, 2014, [Online]. Available: http://www.jurnaljam.ub.ac.id/index.php/jam/article/view/711.

[9] KOMINFO, *Panduan Umum Tata Kelola Teknologi Informasi Nasional*. 2007.

[10] E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, "Information security assessment in public administration," *Comput. Secur.*,

vol. 90, 2020, doi: 10.1016/j.cose.2019.101709.

[11] M. Rhodes-Ousley, “The Complete Information Security Second Edition,” 2013, p. 897.

[12] M. K. dan I. R. Indonesia, *Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi*. 1393, p. 93.

[13] J. Zarei and F. Sadoughi, “Information security risk management for computerized health information systems in hospitals: A case study of Iran,” *Risk Manag. Healthc. Policy*, vol. 9, pp. 75–85, 2016, doi: 10.2147/RMHP.S99908.

[14] W. Syafitri, “Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ),” *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 2, no. 2, p. 8, 2016, doi: 10.24014/coreit.v2i2.2356.

[15] P. Shedden, A. Ahmad, W. Smith, H. Tscherning, and R. Scheepers, “Asset identification in information security risk assessment: A business practice approach,” *Commun. Assoc. Inf. Syst.*, vol. 39, no. 1, pp. 297–320, 2016, doi: 10.17705/1cais.03915.

[16] R. V. Imbar and A. E. Ayala, “PENERAPAN STANDAR KEAMANAN INFORMASI MENGGUNAKAN FRAMEWORK ISO/IEC 27005:2011 di LAPAN BANDUNG,” *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 1, pp. 195–206, 2018, doi: 10.28932/jutisi.v4i1.770.

[17] M. Al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, “Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency,” *Procedia Comput. Sci.*, vol. 161, pp. 1206–1215, 2019, doi: 10.1016/j.procs.2019.11.234.

[18] R. R. Putra, “ANALISIS MANAJEMEN RISIKO TI PADA KEAMANAN DATA E - LEARNING DAN ASET IT MENGGUNAKAN NIST SP 800 – 30 Revisi 1,” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 6, no. 1, pp. 96–105, 2019, doi: 10.35957/jatisi.v6i1.154.

[19] S. Ariyani and M. Sudarma, “Implementation Of The ISO / IEC 27005 In Risk Security Analysis Of Management Information System,” vol. 6, no. 8, pp. 1–6, 2016.

[20] F. A. Anshori and A. R. Perdanakusuma, “Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 2, pp. 1701–1707, 2019, [Online]. Available: http://j-ptiik.ub.ac.id.

[21] ISO/IEC, “ISO/IEC 27002:2013.pdf,” *Iec*, vol. 2013. p. 90, 2013, [Online]. Available: www.iso.org.

[22] F. Fouad, “Information Security Risk Plans within Enterprise Architecture Framework,” *Int. J. Adv. Comput. Sci. Technol.*, vol. 8, no. 10, pp. 32–40, 2019, doi: 10.30534/ijacst/2019/018102019.

[23] I. T. Informasi, “Design of Risk Management Based on Information Security,” vol. 1, 2020.

[24] M. Utomo, A. Holil, N. Ali, and I. Affandi, “Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I,” *J. Tek. Its*, vol. 1, no. 1, pp. 2–7, 2012, [Online]. Available: http://ejurnal.its.ac.id/index.php/teknik/article/viewFile/900/462.

[25] T. Kristanto, R. Arief, and N. F. Rozi, “Perancangan Audit Keamanan Informasi Berdasarkan Standar Iso 27001:2005 (Studi Kasus: PT. Adira Dinamika Multi Finance),” *Semin. Nas. Sist. Inf. Indones. 22 Sept. 2014*, vol. 2005, no. October 2015, pp. 1–6, 2014.

[26] E. Lomas, “Information governance: Information security and access within a UK context,” *Rec. Manag. J.*, vol. 20, no. 2, pp. 182–198, 2010, doi: 10.1108/09565691011064322.

[27] T. K. Priyambodo and Y. Prayudi, “Information security strategy on mobile device based egovernment,” *ARPN J. Eng. Appl. Sci.*, vol. 10, no. 2, pp. 652–660, 2015.

[28] A. Asriyanik and Prajoko, “Manajemen Keamanan Informasi pada Sistem

Informasi Akademik Menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 315–325, 2018, doi: 10.28932/jutisi.v4i2.792.

[29] NIST, "NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments," *NIST Special Publication*, no. September. p. 95, 2012, doi: 10.6028/NIST.SP.800-30r1.

[30] S. M. Jaya, "Perancangan Sistem Keamanan Informasi Berbasis Penilaian Resiko Menggunakan ISO/IEC 27001 Dan ISO/IEC 27005 (Studi Kasus: Kajian Teoritis)," *E-Journal.Umc.Ac.Id*, vol. 27005, pp. 12–22, [Online]. Available: https://e-journal.umc.ac.id/index.php/INT/article/view/370.

[31] M. Zammani and R. Razali, "An empirical study of information security management success factors," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 6, no. 6, pp. 904–913, 2016, doi: 10.18517/ijaseit.6.6.1371.

[32] R. E. G. Fajar Ilham Satria Yudha, "RISK ASSESSMENT PADA MANAJEMEN RESIKO KEAMANAN INFORMASI MENGACU PADA BRITISH STANDARD ISO/IEC 27005 RISK MANAGEMENT," *Appl. Catal. A Gen.*, vol. 58, no. 2, pp. 15–22, 2013, doi: 10.1179/1743280412Y.0000000001.

[33] R. Hoffmann, M. Kiedrowicz, and J. Stanik, "Risk management system as the basic paradigm of the information security management system in an organization," *MATEC Web Conf.*, vol. 76, 2016, doi: 10.1051/matecconf/20167604010.

[34] E. Technologies, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security for supplier relationships —," vol. 2014. 2014.

[35] R. Sanchez and J. Enrique, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security," vol. 2016, 2017.

[36] V. Agrawal, "Towards the Ontology of ISO/IEC 27005:2011 risk management standard," *Proc. 10th Int. Symp. Hum. Asp. Inf. Secur. Assur.*

HAISA 2016, no. Haisa, pp. 101–111, 2016.

[37] O. B. Umum, “Direktorat Penelitian dan Pengaturan Perbankan,” no. November. p. 2009, 2007.

[38] WALIKOTA SURAKARTA and P. J. TENGAH, “PERATURAN WALIKOTA SURAKARTA NOMOR 28 TAHUN 2019 TENTANG PEDOMAN PENYELENGGARAAN E-GOVERNMENT,” vol. 8, no. 2. p. 2019, 2019, doi: 10.22201/fq.18708404e.2004.3.66178.

LAMPIRAN

Bentuk kuesioner yang digunakan

Cara Pengisian Kuesioner :

1. Mohon mengisi kolom yang ada pada kolom 5 yaitu **kecenderungan**, kolom 6 yaitu **dampak** dan kolom 8 yaitu **pengendalian yang ada**
2. Kolom 5 di isi dengan pilihan urut yang dimulai dengan frekuensi yang hampir tidak pernah terjadi (pilih salah satu)
3. Kolom 6 di isi dengan pilihan yang urut dimulai dengan dampak yang paling kecil (pilih salah satu)
4. Kolom 8 di isi dengan kegiatan atau kebijakan yang dimiliki organisasi yang dapat memperkecil dampak dari resiko

Kuesioner Penilaian Resiko
Aset Perangkat IT

NO	Klasifikasi Aset		Identifikasi Resiko		Analisa Resiko			
		Aset	Resiko	Kerawanan	Kecenderungan	Dampak	Nilai Resiko	Pengendalian yang ada
	1	2	3	4	5	6	7	8

serviens in lumine veritatis

Bentuk Penilaian Kecenderungan

Likelihood		**Deskripsi**	**Frekuensi Terjadi**
Level	**Kriteria**		
1	*Rare*	Hampir tidak pernah terjadi	>2 tahun
2	*Unlikely*	Kemungkinan terjadi ada tetapi kecil (jarang)	1-2 tahun
3	*Possible*	Mungkin saja terjadi (kadang-kadang)	7-12 bulan/tahun
4	*Likely*	Kemungkinan besar terjadi (sering)	4-6 bulan/tahun
5	*Almost Certain*	Hampir selalu terjadi	1-3 bulan/tahun

Bentuk Penilaian Dampak

Impact		**Deskripsi**
Level	**Kriteria**	
1	*Very Low*	Tidak menyebabkan gangguan yang signifikan pada operasional bisnis. Penyelesaian dilakukan sampai 7 hari
2	*Low*	Proses bisnis mengalami gangguan yang relatif kecil, namun aktivitas tugas pokok dapat dijalankan secara normal. Penyelesaian dilakukan 1-2 hari
3	*Medium*	Proses bisnis mengalami gangguan yang menyebabkan sebagian bisnis mengalami penundaan. Penyelesaian masalah dilakukan paling lama 1 hari
4	*High*	Proses bisnis mengalami gangguan yang relatif besar yang menyebabkan aktivitas bisnis mengalami penundaan. Penyelesaian masalah dilakukan kurang dari 12 jam
5	*Very High*	Proses bisnis mengalami gangguan total yang berdampak krusial yaitu hingga keseluruhan proses bisnis tidak tercapai. Penyelesaian masalah ini harus dilakukan kurang dari 1 jam

Nilai Risiko

Kecenderungan-Dampak	Level Risiko
1,1	*Low*
1,2	*Low*
1,3	*Low*
1,4	*Medium*
1,5	*Medium*
2,1	*Low*
2,2	*Low*
2,3	*Medium*
2,4	*Medium*
2,5	*High*
3,1	*Low*
3,2	*Low*
3,3	*Medium*
3,4	*High*
3,5	*High*
4,1	*Low*
4,2	*Medium*
4,3	*High*
4,4	*High*
4,5	*High*
5,1	*Medium*
5,2	*Medium*
5,3	*High*
5,3	*High*
5,5	*High*

Daftar Aset Perangkat IT

No	Data Aset				Spesifikasi Aset	
	Nama Aset	Nomor Aset	Nomor Registrasi	Penanggung Jawab	Merk	Tahun Pembelian
1	Alat Komunikasi Sosial (Streaming Radio Anak)	02.07.02.06.04	0002	Pengurus Barang	-	2016
2	Kamera + Attachment	02.07.01.01.01	0002	Pengurus Barang	1. Mirrorless Fujifilm/ X-T10 2.Fujifilm/ XT2 Pro Kit 3. Fujifilm/ Mirrorless Digital C	2015, 2017
3	Drone	02.06.01.05.04	0106	Pengurus Barang	1. Panthom/ 3 Profesional 2.Drone Yuneec/ Thypoon 500	2016
4	Handycam	02.06.02.06.49	0002	Pengurus Barang	Sony HDR/ PJ 340	2014
5	Jaringan FOC dan LAN Balai Kota	02.07.01.05.03	0002	Pengurus Barang	-	2016
6	Laptop/ Notebook	02.06.03.02.02	0016-0018 0030-0044	Pengurus Barang	1. Lenovo 2. Apple 3. Tablet Apple 4. Asus 5. HP/ Pavilion 6. Macbook/ Pro MLH12	2006, 2015, 2017

7	LCD Projector	02.06.01.05.42	0005-0008	Pengurus Barang	1. NEC/ M403WG 2. Panasonic/ VW430EA	2016
8	Lensa Kamera	02.07.01.02.63	0003-0005	Pengurus Barang	1. Fujinon/ XF50- 140 MM GSPL 2. Mirrorless Fujifilm Finepix X-T1 Lensa 18-135 3. Canon/ DSLR Canon 7D Mark II	2016, 2017
9	Memori Kamera	02.07.01.02.00	0008-0009	Pengurus Barang	Sandisk	2017
10	PC Komputer	02.06.03.02.01	0014-0032	Pengurus Barang	1. Processsor Intel/ i3-4150 (3.5 Ghz-C/3MB) 1150 2. Acer 3. HP Compaq 4. Lenovo/ AIO 720 5. Lenovo/ AIO PC510-crid	2011, 2016, 2017
11	Peralatan SMS Hotline	02.06.03.06.06	0119	Pengurus Barang	-	2012
12	Peralatan Jaringan Komputer (Pemindahan/ Integrasi LPSE ke DISHUBKOMINFO)	02.06.03.06.06	0120	Pengurus Barang	-	2012

13	Printer	02.06.03.05.03	0003- 0014	Pengurus Barang	1. Epson/ L220 2. Canon/ MP 258 3. Canon/ MP 276 4. Epson, Epson/ M200 5. Epson/ L565 6. Epson/ L365	2009, 2011, 2016, 2017
14	Scanner	02.04.03.07.10	0002-0004	Pengurus Barang	1. HP 2. Scanner Lide	2009, 2011, 2016
15	Telephone PABX	02.07.02.01.09	0001-0002	Pengurus Barang	-	2015
16	TV	02.06.01.05.40	0001 0062- 0101 0107- 0122	Pengurus Barang	1. Sharp Aquos 32” 2. Samsung	2015, 2015, 2017
17	Server	02.06.03.06.06	0124	Pengurus Barang	IBM SYSTEM / X3650 M5	2015
18	UPS	02.06.03.05.11	0001-0002	Pengurus Barang	UPS Rack Mount/ 5000 VA	2017

Risk Register Aset Perangkat IT

No	Klasifikasi Aset	Identifikasi Risiko			Analisis Risiko			
		Aset	**Risiko**	**Kerawanan**	**Kecenderungan**	**Dampak**	**Nilai Risiko**	**Pengendalian yang ada**
1.	Alat Pemroses Data	- Jaringan FOC dan LAN Balai Kota - Peralatan Jaringan Komputer (Pemindahan/ Integrasi LPSE ke DISHUBKOMINFO)	Kerusakan pada switch atau hub	Sistem pengamanan perangkat lunak tidak diperbarui secara berkala, port yang tidak digunakan masih aktif	1	3	1,3	
			Kerusakan peralatan	-Kurangnya pelaksanaan pemeliharaan secara berkala -Tidak adanya prosedur pergantian alat secara berkala	1	4	1,4	
			Kesalahan penggunaan	Tidaknya dokumentasi user	1	2	1,2	

				manual untuk penggunaan alat				
			Terjadinya hubungan arus pendek	Aliran listrik yang tidak stabil	3	3	3,3	Organisasi menggunakan stabilizer
			Pencurian/Kehilangan	Lokasi yang terbuka dan tidak memiliki pelindung atau pengaman khusus	5	2	5,2	Organisasi rutin melakukan jumat bersih
2.	Peralatan Portabel	- Laptop/ Notebook - Kamera + Attachment - Handycam	Peralatan eror	Terdapat virus karena penggunaan alat yang tidak diperhatikan	4	2	4,2	Bidang informatika mewajibkan untuk service inter setiap peralatan
			Power failure	Ketersediaan listrik yang tidak stabil	1	1	1,1	Organisasi memiliki genset yang selalu standby

			Penyalahgunaan hak akses	-Tidak ada pencatatan dan pengawasan log penggunaan alat	4	3	4,3	
			Pencurian	Kualitas keamanan organisasi yang kurang maksimal	1	2	1,2	Tempat penyimpanan peralatan diawasi cctv 24 jam
			Kerusakan	-Maintenance yang kurang baik dan tidak teratur -Penggunaan yang tidak tepat	1	1	1,2	
3.	Peralatan Tetap	- PC Komputer - Telephone PABX - Tv - Printer - Server	Power failure	Ketersediaan listrik yang tidak stabil	1	1	1,1	Organisasi memiliki genset yang selalu standby
			Bencana alam	Peletakan peralatan ada di tempat yang rawan bencana	1	5	1,5	

			Denial of Service	Terdapat kerentanan terhadap sistem keamanan server	1	3	1,3	
			Server Down	Pengguna server yang terlalu banyak dalam satu waktu	1	2	1,2	Organisasi memiliki backup server tersendiri
			Kebakaran	Adanya aliran arus pendek/korsleting	1	2	1,2	Organisasi menggunakan sprinkle water system
			Debu dan kotoran	Kerentanan terhadap debu dan kotoran karena letak peralatan yang tidak sesuai ketentuan	1	2	1,2	Organisasi mempunyai kegiatan rutin jumat bersih-bersih
			Human Eror	Kurangnya pelatihan proses pada pengguna alat/IT	1	2	1,2	Organisasi melakukan pelatihan rutin

4.	Pengolah perifer	- Scanner - Alat Komunikasi Sosial (Streaming Radio Anak) - Drone - LCD Projector - Peralatan SMS Hotline	Alat Eror	Kerentanan alat terhadap kelembaban, debu dan kotoran	1	1	1,1	
			Kerusakan alat	Maintenance yang kurang baik dan tidak dilakukan secara teratur	1	2	1,2	
			Pencurian	Kualitas keamanan organisasi yang kurang maksimal	1	2	1,2	Tempat penyimpanan peralatan diawasi cctv 24 jam
			Kesalahan penggunaan alat	Organisasi tidak memiliki dokumentasi manual untuk penggunaan alat	1	3	1,3	
			Penyalahgunaan hak akses	Tidak ada pembatasan hak	1,	3	1,3	

				akses pada setiap alat				
5.	Media data(pasif)	- Memori Kamera	Data corrupt	Perlindungan terhadap file tidak diperhatikan dengan baik	1	3	1,3	
			Penyimpanan penuh	Tidak adanya pemindahan data secara berkala	1	1	1,1	Organisasi menyediakan penyimpanan data berupa hardisk terpisah untuk data dari liputan
			Kehilangan	Kurangnya pengawasan dan keamanan pada penyimpanan	1	1	1,1	1.Terdapat pembatasan akses masuk ke ruangan-ruangan tertentu 2. Keamanan menggunakan

								sidik jari 3. Terdapat kamera keamanan
			Kerusakan	Tempat penyimpanan yang tidak sesuai dengan standar	1	1	1,1	
6.	Media elektronik	- UPS	Baterai pada ups tidak dapat menyimpan daya	UPS terlalu banyak beban untuk melakukan cover dari perangkat lunak yang melebihi dari ketentuan	1	2	1,2	
			Kerusakan ups	Lokasi dan lingkungan penyimpanan yang tidak sesuai standar	1	1	1,1	

			Kehilangan ups	Sistem pengamanan yang tidak maksimal	1	1	1,1	

Penilaian Risiko

No	Klasifikasi	Aset	Risiko	Nilai risiko (kecenderungan, dampak)
	1	2	3	4
1	Alat Pemroses Data	- Jaringan FOC dan LAN Balai Kota - Peralatan Jaringan Komputer (Pemindahan/ Integrasi LPSE ke DISHUBKOMINFO)	Kerusakan pada switch atau hub	1,3/*Low*
			Kerusakan peralatan	1,4/*Medium*
			Kesalahan penggunaan	1,2/*Low*
			Terjadinya hubungan arus pendek	3,3/*Medium*
			Pencurian/Kehilangan	5,2/*Medium*
2	Peralatan Portabel	- Laptop/ Notebook - Kamera + Attachment - Handycam	Peralatan eror	4,2/*Medium*
			Power failure	1,1/*Low*
			Penyalahgunaan hak akses	4,3/*High*
			Pencurian	1,2/*Low*
			Kerusakan	1,2/*Low*
3	Peralatan Tetap	- PC Komputer	Power failure	1,1/*Low*

		- Telephone PABX - Tv - Printer - Server	Bencana alam	1,5/*Medium*
			Denial of Service	1,3/*Low*
			Server Down	1,2/*Low*
			Kebakaran	1,2/*Low*
			Debu dan kotoran	1,2/*Low*
			Human Eror	1,2/*Low*
4	Pengolah perifer	- Scanner - Alat Komunikasi Sosial (Streaming Radio Anak) - Drone - LCD Projector - Peralatan SMS Hotline	Alat Eror	1,1/*Low*
			Kerusakan alat	1,2/*Low*
			Pencurian	1,2/*Low*
			Kesalahan penggunaan alat	1,3/*Low*
			Penyalahgunaan hak akses	1,3/*Low*
5	Media data(pasif)	- Memori Kamera	Data corrupt	1,3/*Low*
			Storage penuh	1,1/*Low*
			Kehilangan	1,1/*Low*
			Kerusakan	1,1/*Low*
6	Media elektronik	- UPS	Baterai pada ups tidak dapat menyimpan daya	1,2/*Low*
			Kerusakan ups	1,1/*Low*

			Kehilangan ups	1,1/*Low*

Tabel Rekomendasi

No	Klasifikasi	Aset	Risiko	Nilai risiko (kecenderungan, dampak)	Rekomendasi
	1	2	3	4	
1	Alat Pemroses Data	- Jaringan FOC dan LAN Balai Kota - Peralatan Jaringan Komputer (Pemindahan/ Integrasi LPSE ke DISHUBKOMINFO)	Kerusakan pada switch atau hub	1,3/*Low*	Membuat pelindung khusus untuk alat-alat yang rentan dengan kerusakan seperti kabel
			Kerusakan peralatan	1,4/*Medium*	Pembuatan user manual book dan pemberian pelatihan secara berkala pada SDM
			Kesalahan penggunaan	1,2/*Low*	Melakukan pelatihan user ketika terjadi pembaharuan alat
			Terjadinya hubungan arus pendek	3,3/*Medium*	Memaksimalkan stabilizer yang sudah ada

			Pencurian/Kehilangan	5,2/*Medium*	meningkatkan keamanan organisasi, dengan melakukan pengecekan secara berkala pada ketersediaan alat
2	Peralatan Portabel	- Laptop/ Notebook - Kamera + Attachment - Handycam	Peralatan eror	4,2/*Medium*	Melakukan maintenance secara berkala, melakukan pengadaan alat yang sesuai standar
			Power failure	1,1/*Low*	Menambahkan *stabilizer* tegangan listrik.
			Penyalahgunaan hak akses	4,3/*High*	Membuat catatan log untuk setiap penggunaan aset dan disetujui oleh pihak yang berwenang

			Pencurian	1,2/*Low*	meningkatkan keamanan organisasi, dengan melakukan pengecekan secara berkala pada ketersediaan alat
			Kerusakan	1,2/*Low*	Melakukan penyuluhan berkala mengenai pemeliharaan aset agar aset terjaga dalam jangka panjang
3	Peralatan Tetap	- PC Komputer - Telephone PABX - Tv - Printer - Server	Power failure	1,1/*Low*	Memaksimalkan penggunaan genset, melakukan pengecekan secara berkala
			Bencana alam	1,5/*Medium*	Membuat skenario bencana, Meletakan aset-aset kritikal di tempat yang lebih tinggi.

			Denial of Service	1,3/*Low*	Menggunakan sistem keamanan/firewall yang sesuai standar dan Memblokir layanan-layanan dan situs yang berbahaya
			Kebakaran	1,2/*Low*	Membuat skenario bencana, Meletakan aset-aset kritikal di tempat yang lebih tinggi. Menjauhkan aset-aset kritikal dari pemicu api tercepat.
			Debu dan kotoran	1,2/*Low*	Memberikan pelindung dan rutin melakukan pembersihan alat
			Human Eror	1,2/*Low*	Pembuatan *user manual book* untuk pengguna

					yang mampu meminimalisir risiko
4	Pengolah perifer	- Scanner - Alat Komunikasi Sosial (Streaming Radio Anak) - Drone - LCD Projector Peralatan SMS Hotline	Alat Eror	1,1/*Low*	Menyediakan lisensi perangkat IT yang asli dan aman kepada pengguna.
			Kerusakan alat	1,2/*Low*	Melakukan penyuluhan berkala mengenai pemeliharaan aset agar aset terjaga dalam jangka panjang
			Pencurian	1,2/*Low*	meningkatkan keamanan organisasi, dengan melakukan pengecekan secara berkala pada ketersediaan alat
			Kesalahan penggunaan alat	1,3/*Low*	Membuat *user manual book*, memberikan pelatihan secara berkala

					untuk setiap pembaharuan aset
			Penyalahgunaan hak akses	1,3/*Low*	Membuat catatan log untuk setiap penggunaan aset dan disetujui oleh pihak yang berwenang
5	Media data(pasif)	Memori Kamera	Data corrupt	1,3/*Low*	Melakukan *update* secara berkala aplikasi antivirus, melakukan *scanning* secara rutin
			Storage penuh	1,1/*Low*	Melakukan pemindahan data secara langsung setelah pemakaian
			Kehilangan	1,1/*Low*	Membuat catatan log akses pengunjung pada lokasi aset bertempat.
			Kerusakan	1,1/*Low*	Melakukan penyuluhan berkala mengenai pemeliharaan aset agar

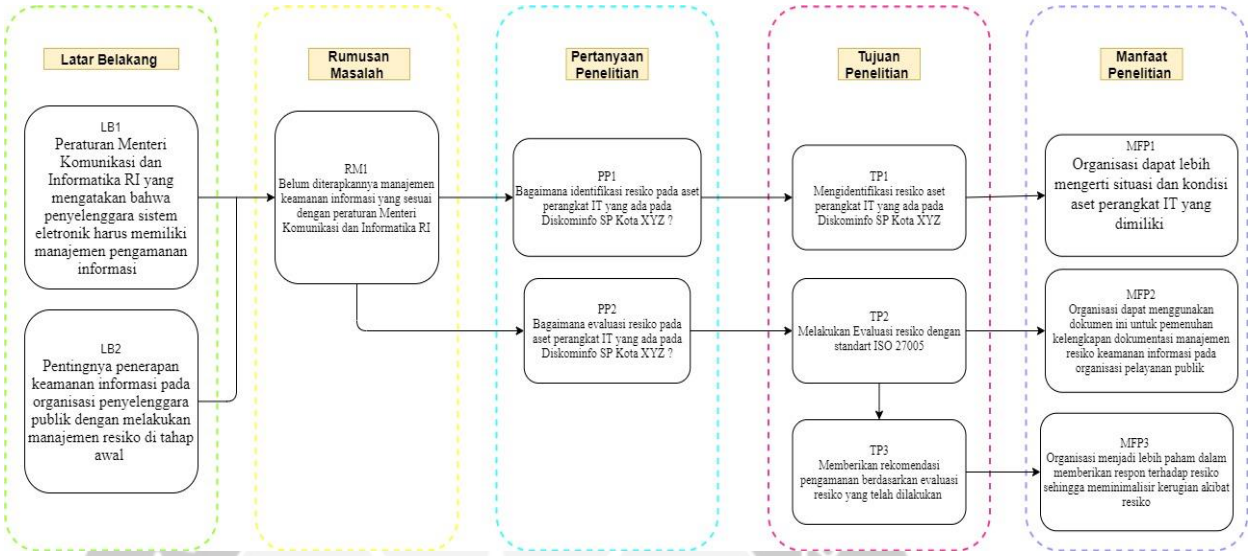
					aset terjaga dalam jangka panjang
6	Media elektronik	UPS	Baterai pada ups tidak dapat menyimpan daya	1,2/*Low*	Melakukan pengecekan alat secara berkala, melakukan pengadaan sesuai
			Kerusakan ups	1,1/*Low*	Melakukan penyuluhan berkala mengenai pemeliharaan aset agar aset terjaga dalam jangka panjang melakukan penggantian alat secara berkala
			Kehilangan ups	1,1/*Low*	meningkatkan keamanan organisasi, dengan melakukan pengecekan secara berkala pada ketersediaan alat

REVISI

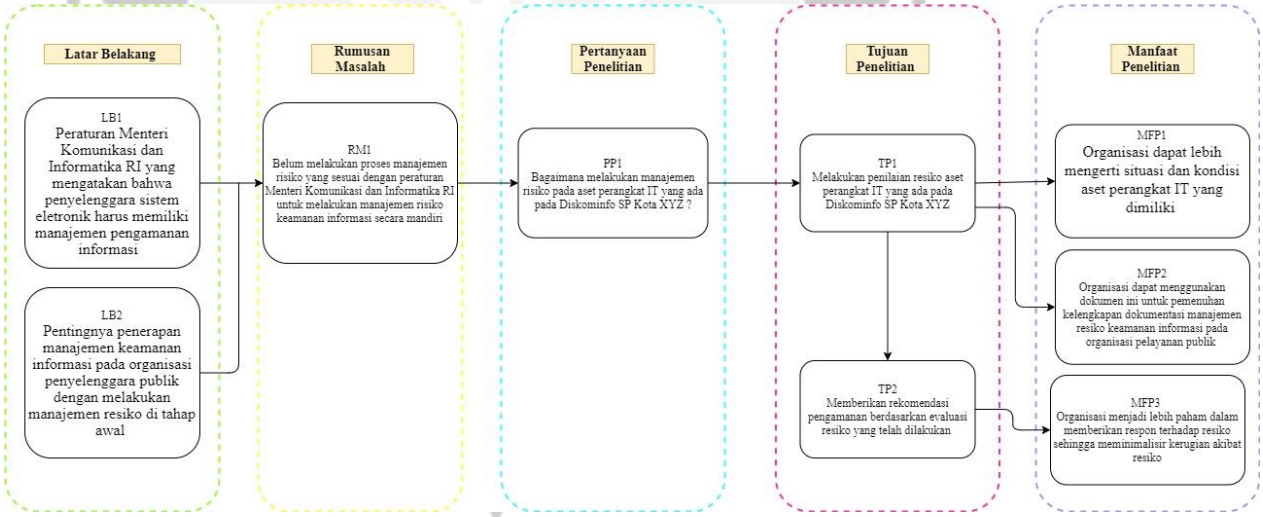
No.	Revisi	Halaman
1.	Gap dari rumusan masalah ke pertanyaan penelitian	Hal.6(bagan keterkaitan)
2.	Bagaimana proses munculnya nilai resiko dan dampak?	Hal.29(Penilaian risiko)
3.	Bagaimana proses perumusan rekomendasi? Dari km sendiri atau dr pakar?	Hal. 29(Rekomendasi)
4.	Apakah sudah ada approval dari pihak kominfo ttg dokumen resiko dan rekomendasimu ini?	36
5.	Sejauh mana diskominfo sudah peduli terhadap resiko2 IT? Apa saja upaya2 diskominfo dalam menumbuhkan budaya peduli resiko?	Hal. 3
6.	apa itu resiko? Apa saja kategori2 resiko? Dan mengapa resiko harus dimanage?	Hal.14 dan 16
7.	Tambahkan cara/metoda bagaimana penghitungan resiko di bgaian metodologi	Hal.29
8.	Pemanggilan setiap tabel dan gambar	Telah diperbaiki
9.	Typo dan italic	Telah diperbaiki

Bagan Keterkaitan

Bagan lama



Bagan baru



serviens in lumine veritatis